International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(15s) 2026 pp. 150-160
https://doi.org/10.70917/ijcisim-2026-4382
Article

A REVIEW OF AUTHENTICATION MECHANISMS IN INDIA'S DIGITAL PAYMENT ECOSYSTEM: FROM OTP TO BEHAVIOURAL BIOMETRIC, IN LIGHT OF RBI'S 2025 AUTHENTICATION DIRECTIONS

Divyaraj Parmar[1], Pankaj Rathod[2], Vatsal Chandrapal[3], Khyati Kariya[4]

[1]Parul University, Vadodara, India, 2305112120080@paruluniversity.ac.in, https://orcid.org/0009-0008-4097-7445
[2]Parul University, Vadodara, India, 2305112110030@paruluniversity.ac.in, https://orcid.org/0009-0008-6755-889X
[3]Parul University, Vadodara, India, 2305112110006@paruluniversity.ac.in, https://orcid.org/0009-0003-4571-3979
[4]Parul University, Vadodara, India, khyati.kariya33400@paruluniversity.ac.in, https://orcid.org/0009-0007-3458-6539

Abstract: Digital payment, a journey of tremendous growth in India, from the inception of Unified Payments Interface, card-not-present transactions, mobile banking, prepaid payment products, Aadhaar services and merchant digitisation. The scale and convenience that this expansion brings have rendered authentication a key governance and security concern as it can open up opportunities for account takeover, phishing, social engineering, SIM-swap fraud, device compromise, and transaction manipulation. The Reserve Bank of India (RBI) has issued directions on authentication for 2025 that mark a significant shift from a one-time password (OTP) driven authentication system based on SMS to a more comprehensive, principles-based and risk-sensitive authentication framework. The directions continue to mandate two factor authentication for the majority of digital payments transactions, but add the requirement for at least two authenticating factors for digital payments transactions (non-card-present) and at least one dynamic or provable factor for digital payments transactions that are not card-present. They also enable more risk based checks depending on the context of the transactions, as well as the perception of fraud, but not any one specific technical pathway.

This paper discusses the different type of authentication models that have been developed in India, ranging from pin, otp, biometric to behavioural biometric model and its regulatory, technical and operational implications as per the directions issued in 2025. A comparative analysis of the regulatory materials is carried out and a doctrinal and analytical review methodology is applied which takes into account all the authentication factors (knowledge, possession, inherence, contextual intelligence) with the most recent security discourse. The results section is designed in a manner that allows for comparison of the mainstream methods based on the strength of the security, ease of use, deployability, resistance to fraud, impact on privacy visibility and regulatory fit in the RBI context.

The paper concludes that OTP-based systems are also important, but also become increasingly inadequate as a solution to today's frauds, due to their susceptibility to interception, manipulation, and social engineering. While not ideal, behavioural biometric systems provide a strong second line of risk scoring, anomaly detection and adaptive authentication. What will work best for India is not simply to replace OTP with biometrics with a single model, but a multi-layered model where aspects of dynamic authentication, device intelligence, behavioural signals and transaction risk analytics all play a part within a standards-based interoperable compliance regime. The RBI guidelines underscore the importance of transitioning towards the adaptive trust mechanism rather than phasing out the existing mechanism for digital transactions.

Keywords: India digital payments, authentication mechanisms, OTP, behavioural biometric, RBI 2025 directions, two-factor authentication, UPI security, card-not-present payments, risk-based authentication, digital financial regulation

1. Introduction

1.1 Background of India's digital payment transformation

India has emerged as one of the biggest digital payment markets in the world. Public digital infrastructure, affordable Smartphones, prevalence of the internet, QR code payment acceptance, fintech innovation, and the move towards formalised digital transactions have changed it. UPI has altered the landscape of P2P and P2M payment transactions, and the growing number of card-based e-commerce, mobile wallet, prepaid instruments and mobile banking applications have added to the range of digital payment channels for consumers and merchants (Saini, 2025). This shift has resulted in distinct improvements in terms of transactions visibility, speed, access and traceability. In the meantime it has turned into an important security link.

Digital payments aren't just a technical process that precedes authorisation. It is one way in which trust is put into practice. The truth is that authentication is used to determine if a particular user is legitimate, if a device is known or suspected, if a transaction is normal or not, and whether the use of a payment rail is considered to be at an acceptable risk of fraud. Authentications should function in a market as large and varied as India, where the devices are not all created equal, language barriers, lack of digital literacy, telecom networks, and processes also differ. This is especially true for academic/regulatory research in India.

1.2 Authentication as a policy and security challenge

What is difficult in India is not that there is no authentication, but that some aspects are stressed on a few methods that have been known. For years, the ecosystem has been dependent on various combinations, like card details and OTP, mobile application login and MPIN, and account access and registered device assumptions. The models were adequate for a period when the first goal was to create a safety foundation adoption. However, eventually, the techniques for defrauding became more sophisticated (Vidani, 2024). Instead of brute force attacks, more advanced attacks were implemented, including phishing, remote screen sharing, social engineering, malicious apps, SIM swapping, and mule routing and convincing fake consent flows. But there could still be a role for a mechanism such as SMS OTP in such an environment, just not a security responsibility alone.

The regulatory approach has slowly shifted from prescriptive minimum safeguards to a more complex notion of layered and contextual control. The RBI's 2025 authentication guidelines are important as they capture this transition as well. They maintain their basic two-factor authentication structure (which means that most digital payment transactions require two different types of factors for authentication), and add a clearer separation between the types of factors, and make more stringent requirements for non-card-present transactions by requiring at least one factor to be dynamic or verifiable. Furthermore, they enable additional fraud risk checks. With this architecture, regulators will have more space to integrate in biometrics, device-native verification, risk engines and behavioural analytics, all while maintaining a focus on issuers and payment participants.

1.3 Research problem

One of the significant challenges this paper attempts to address is the digital payment ecosystem being created in India is outstripping the legacy payment assumption of authentication. OTP is deeply integrated in transaction flows, due to its low price, familiarity, interoperability and regulatory acceptance. But new methods of fraud exploit the human and infrastructural vulnerabilities in the process of delivery of OTPs. The Biometrics are user-binding but are less convenient due to false acceptance, device inequality, consent, privacy, and spoofing and irrevocability (Khan, 2023). Whilst behavioural biometrics are continuous and frictionless verification, they present a number of challenges, including the lack of transparency, surveillance concerns, data governance issues, and inconsistent legal development.

The research question is not just if behavioural biometrics are better than OTP. The more pressing question is how India's payment system in the RBI's vision for 2025 can be designed to enable multiple layers of authentication, as well as to take into account security, inclusion, convenience, interoperability and proportionality.

1.4 Research objectives

This paper is designed to have four aims. The first one is moving towards OTP to biometric and behavioural authentication in India's digital payment system.The first one is the transition from OTP-based authentication to biometric and behavioural authentication in India's digital payment system.The first one is a shift from an OTP authentication model to biometric and behavioural authentication in India's digital payment system. The second is to ensure that the directions of RBI regarding the authentication gets translated into regulation by 2025. The third is to

evaluate the main authentication techniques in terms of security, usability, privacy and implementation. The fourth is to highlight a realistic design path for authentication in near future that is not just fraud-resistant, but also provides access for consumers in India.

1.5 Scope of the study

The paper emphasizes on various aspects of digital payment authentication in the retail segment in India including domestic digital payment transactions, card-not-present transactions, mobile banking, wallets, UPI transactions and implications of risk-based controls. It does not provide a comprehensive analysis of all the circulars released by the RBI over the last decade or attempt to cover the entire payment infrastructure in wholesale payments. It also does not attempt to offer main empirical fraud measurements from regulated entities (Khan, 2023). The contribution is analytical and review in nature with focus on the importance of the directions for 2025 and what they mean for authentication design.

2. Conceptual Foundations of Digital Payment Authentication

2.1 Meaning and function of authentication

Authentication is the process of verifying a user, device or transaction claim. In digital payments the authentication is between identity and authorisation. Who is speaking: "I am...". Authentication asks if the claimant is someone who is likely to be the actual claimant. Authorisation is a determination whether the authenticated person is authorized to make the transaction. These layers can be fused together, and ultimately result in payment security problems. The authentication part may be weak or compromised, but the customer account could be legitimate and the transaction could be fraudulent.

2.2 Classical categories of authentication factors

There are 3 types of authentication factors that can be classified from the aspect of a payment and information security. The first is something that the user is able to recall like a password, PIN, pass phrase, or challenge answer. The second is an object that the user possesses, such as a card, device, token, crypto application or OTP receipt capability. The third is a property of the user, such as a fingerprint, face, iris, voice or other biometric property. The RBI's framework for 2025 makes it abundantly clear that it leaves this factor-based framework intact and also requires a separate factor and not the same factor in multiple forms.

2.3 Dynamic, proven, and contextual authentication

The difference between static and dynamic trust is the major conceptual development in the current phase. Static methods use credentials that have been set up beforehand, like a stored password or remembered device. With Dynamic methods, evidence is created or confirmed when the transaction occurs (Quraishy, 2026). The OTP is dynamic because as expected, it is only to be used for one single transaction or session. A biometric is deemed to be proved if at the time it is required the system requires the presentation of the biometric and a strong matching of the biometric. Contextual and behavioural methods are based on these, and are used to analyze device fingerprint, the consistency of geolocation data, session behavior, typing rhythm, typing pressure, swipe pattern, navigation cadence, transaction history and markers for anomalies. These signals may not be apparent to the end user, but they will have an impact to the level of authentication confidence.

3. Evolution of Authentication in India’s Digital Payment Ecosystem

3.1 Early emphasis on PINs, passwords, and card credentials

Initial digital payments models in India were based on the fundamental knowledge-based and possession-based associations. Use of debit and ATM involves cards and pin numbers. Internet banking was based on passwords, transaction passwords and challenge questions. The card number was an added factor along with expiry and CVV along with more recently OTP with the launch of card-not-present commerce (CNP). Such systems were better than single password systems for security, but had some weaknesses. Users credentials were stolen and reused; merchants set up sensitive data in an insecure manner; attackers captured static data by phishing and malware.

3.2 Rise of SMS OTP as the dominant additional factor

OTP emerged as the most prominent brand of secure digital payments in India. It was accepted because of its ease of use and familiarity to users, support of mass-market phones, and ability to be deployed by institutions without

special hardware. OTP also met the regulatory goal of the second factor in addition to using a card or account. In a market where basic telephones were being phased out for smartphones, SMS OTP was a link between the old and new technologies in financial transactions.

But this OTP superiority, bred dependency. It believed that the registered cell phone number would be a good indicator of user's legitimacy (Jyothi, 2025). The assumption weakened as fraudsters started to take advantage of telecom vulnerabilities, SIM replacement, device compromise, message forwarding, fake support calls, malicious overlays, and trick-based customer coercion. Many of the fraud incidents did not involve missing out on OTP, but were deceived into entering the OTP or the malware was able to retrieve the OTP during the SMS sending process.

3.3 Growth of app-based PINs and device binding

The rise in the use of smartphones saw these payment applications add in the features of MPINs, app locks, secure app sandboxes and device binding. Binding to a previously-registered device using identifiers, certificates, cryptographic secrets or signals of platform trust is referred to as device binding. This model minimized the exposure of some credential replay as the payment process increasingly moved to assume that the originating device was important. This has resulted in an increase in the rate of adoption of UPI. Payment instructions might be connected to a user-chosen PIN, to a bank account and to a registered cell phone and the encompassing application security setting.

The device binding process was an attempt to make things more secure, but not to end fraud. It had been disadvantageous toward the device, if it had been infected, coerced, or even remotely controlled. Secondly, device change and number portability caused problems, especially for those with low literacy and rural residents. Security and access were still outstanding.

3.4 Emergence of biometric authentication

Biometric authentication has come in several ways into the ecosystem. In certain systems, one identity stream was introduced with the help of the introduction of Aadhaar based verification using fingerprint/iris. Native fingerprint and facial recognition began to be supported by consumer devices.Consumer devices began supporting native fingerprint and facial recognition. Now, these native capabilities were increasingly being leveraged by payment apps and banking apps for logins, login re-entry and sometimes as transaction confirmation. The benefits of biometric are the high level of user binding as well as reduced memorisation. The finger print approval is quicker for many users compared to PIN authentication and harder to easily share.

Meanwhile, there are governance concerns with biometrics. Biometric attributes can't be modified in case of compromise, unlike passwords. The false match and false rejection impact on trust and usability. Lower end devices will have less powerful sensors. Different kinds of accessibility situations such as elderly users, worn fingerprints on the laborers' fingers, disabled customers, and poor lighting and hardware. Also privacy related issues of storage location, template protection, liveness detection and downstream reuse.

3.5 Transition toward behavioural biometrics and adaptive authentication

The new development in authentication is to rely on the behavior of the user, as well as on his knowledge, possession or identity. Behavioural biometrics is the study of behavior patterns, such as typing speed, touch pressure, gesture angle, hand motion, device usage and transaction speed (Jagannarayan, 2025). The systems are usually operated continuously or semi-continuously, in the background. They don't require a specific challenge for every payment, and instead generate a confidence score. When the behaviour is in line with historical norms, the transaction takes place with low friction. If there are anomalies, the system might ask for another authentication layer, mark the session or deny the payment.

This model is consistent with risk-based regulation as it affords proportional controls. Different low value or routine transactions demand different friction. But not all behavioral deviations should be dealt with by exclusion. The problem is governance: what is the accuracy of the model, is it explainable, is it fair, is it drifting, is it private, etc., etc., there are redress mechanisms.

4. Literature Review

4.1 Global scholarship on payment authentication

This academic research conducted as a whole, makes it clear that the design challenge is to balance security and usability of a digital authentication. Knowledge based factors are easy to make, but can be re-used and can be

guessed or phished. Possession based works better with high integrity devices, but fails with the theft, cloning, interception and telecom compromise. Biometric approaches remove the burden of memory, and make it more convenient for the user, but they also introduce permanence and privacy issues. There are also newer studies that indicate that an adaptive or risk-based authentication system would be a better structure as it would assign friction based on context of the transaction, not every transaction.

The second is related to fraud displacement. If one form of authentication is more prevalent, then the attackers will adapt their actions accordingly. If the system involves the use of OTPs, the attackers are interested in getting the messages and psychological manipulation. Biometric solutions for heavy systems are concerned with bypassing, presentation attack, spoofing and template theft (Bhatnagar *et al*., 2026). This implies that over time, none of these factors is enough.

4.2 Indian literature on digital payments and security

The research on digital payments in India has been limited to digital payment adoption, financial inclusion, diffusion of UPI, trust, and cyber fraud. In all these texts, users have been consistently making the assumption that "OTP" stands for "security" when it really means just that.It is a pattern that has been repeated in all these texts—users think that OTP is about security when it is just about security. Social engineering is one of the major attack vectors identified in digital banking fraud cases in India. It is worth noting that authentication failure can be not only cryptographic, but socio-technical as well.

The second strand of Indian literary works are about Aadhaar, biometric identity and digital governance (Bhatnagar *et al*., 2026). The volume is valuable in that it brings to the fore two perpetual tensions. The first is the battle between scale and consent. The second is the pressure of convenience/exclusion. These findings will be relevant in the context of payment authentication – where a move to a more biometric and/or behavioural business model will raise issues of oversight, transparency and complaints.

4.3 Industry and policy discourse on RBI's 2025 directions

RBI's directions 2025 have drawn convergence with the policy and industry review recently on some points. The directions call for at least two different authentication factors to be used in digital payment transactions unless otherwise exempted. Second, if there is a physical card used at least one factor must be dynamic or provable for digital payment transactions other than paying with a physical card in the presence of the customer. Thirdly, the design does not rule out the use of SMS OTP; but the design makes it less probable that OTP would remain as a de facto design anchor (Kaushik, 2026). Fourth, the second approach allows for the introduction of further checks depending on the risk perceived, thus enhancing the scope of authentication including behavioural and contextual factors. Fifth, compliance for the main framework is on 1st April 2026, with some cross-border card-not-present requirements to come later.

4.4 Research gap

The discussion nowadays is more about compliance and about securing the ecosystem with the new regulations coming into force, but there isn't much integrated discussion going on about the journey of the India's ecosystem from OTP based multi factor authentication to behaviour based biometric and adaptive trust. The material in the existing content is mostly a legal summary and comments on the market or limited technical analysis. There remains a need for a single paper that examines regulatory direction, authentication taxonomy, and ecosystem realities and method for assessment. This research work is a fill in of this.

5. RBI's 2025 Authentication Directions and Their Significance

5.1 Regulatory context

The RBI's instructions to banks for 2025 will be more focused on payment security, while keeping the payments technologic neutral. This framework doesn't require a certain technology stack. Rather, it sets out the results for regulated entities to meet. This is important as India's payment system comprises of different architectures and customer profiles such as banks, fintech, card networks, merchants and payment service providers. If a technology was required, it would have slowed down innovation and increased implementation costs.

5.2 Core requirements

From the doctrinal point of view, the directions might be summarised in the main points. Unless exempted, digital payment transactions must be conducted using two different authentication factors (Saraf, 2024). In any digital payment transaction (excluding card-present physical card use) one or more of the factors will be dynamic or will be able to be proven for that particular transaction. The framework does not yet recognize the knowledge, possession and inherence factors, e.g., OTP, PIN, passphrase, Tokens and Biometrics. Issuers may additionally carry out more checks with the help of risk assessment. Most of the key requirements will need to be met from 1 April 2026 and there are a few exceptions for cross border card-not-present requirements.

5.3 Significance for OTP

This is an important nuance as the directions don't outlaw OTP. When some transaction specific dynamism is needed, OTP is still a valid factor and is still useful. The directions, however, dilute the normative status of OTP as the default unquestioned. From a practical point of view, payment providers can no longer rely on OTP as their universal solution for authentication design (Weerakoon, 2026). They need to question whether the combination of all factors is different, strong, business-connected as appropriate, and immune to damage of one factor leading to the failure of another. This indirectly drives the ecosystem to invest in the following: Device trust, secure App design, Biometric verification, Behavioural risk analytics.

Describe the application of the concept in biometrics and behavioural systems.Explain the significance of the concept in Biometrics and behavioural systems.

The directions are no less significant as they help to confirm a much more different authentication program. This is obviously an inherent characteristic, biometrics. The relevance of the behavioural systems is the extra checks which are included within the framework and based on the risk. Behavioral biometrics is not a second factor itself but it can be combined with the classical second factor and employed to initiate a higher level authentication when some anomaly is detected. The change to the regulation thus dovetails nicely with an adaptive approach, where visible components and hidden contextual controls are combined to yield a control.

6. Methodology

6.1 Research design

In this study, the research method is doctrinal research and analytical research that uses a qualitative approach. It is doctrinal in nature as it explains the directions issued by RBI in 2025 and its implications on regulation. It is analytical, in that it provides a comparison of authentication mechanisms, based on structured criteria that have been derived from payment security practice (Majumdar, 2025). It is also review-based as it gives a synthesis of policy discourse, interpretation of the industry and conceptual literature relevant to the digital payment ecosystem in India.

6.2 Sources of data

There are three types of sources for the paper. These include any regulatory and policy papers on RBI's authentication directions and their effect when put into practice. The second type are recent legal, technology and payments articles by commentators. The third type are conceptual and comparative analysis from the wider body of literature on multi-factor authentication, biometric verification, behavioural analytics and digital payment fraud.

6.3 Analytical framework

Comparisons of authentication mechanisms are carried out under the six evaluative dimensions. The first one is the security that's available to fend off common fraud patterns. The second one is usability or customer friction. Feasibility at the ecosystem level is the third. The fourth exposure is related to privacy and data governance. The fifth one is the ability to withstand phishing and social engineering. The last one is regulatory fit in line with the RBI guidelines of 2025 (Kumar *et al*., 2026). Each method is given a rating on a 5 point scale ranging from 1 – low performance on the dimension and 5 – high performance on the dimension. Not experimental scores and used not as a field measurement but for comparative reasoning.

6.4 Limitations

This paper is not based on bank or payment network proprietary fraud data. This numerical tabulation in the results section is therefore an evaluation and not in the econometric sense. The goal of the study is not to estimate cause but synthesize and compare. Another constraint is that the quality of implementation, training of the models, diversity of devices and governance protections vary between institutions and can have a significant impact on behavioural biometric performance.

7. Results and Analysis

7.1 Comparative assessment of authentication mechanisms

The comparative analysis shows that OTP has moderate-high practical value, but has a decreasing stand-alone adequacy in today's fraud environment. PIN and/or password controls are still required but are relatively ineffective when combined with less effective complementary controls. Device-native biometrics work well on convenience and user binding, but have mixed privacy and inclusion (Jagadisha, 2025). A hardware or software token method works well in terms of cryptographic security, but is more difficult to scale evenly. While the risk-based orchestration and anomaly detection in low friction environments are areas where behavioural biometrics excel, significant transparency, profiling and governance questions remain.

7.2 Numerical Comparison Table

Authentication mechanism	**Security strength (5)**	**Usability (5)**	**Deployability at scale (5)**	**Resistance to phishing/social engineering (5)**	**Privacy exposure risk (5, higher = more risk)**	**Fit with RBI 2025 framework (5)**	**Composite suitability score /30**
Password or static PIN only	2	3	5	1	2	1	14
Card details plus SMS OTP	3	4	5	2	2	4	20
App MPIN plus device binding	4	4	4	3	3	4	22
Device-native fingerprint or face biometric	4	5	4	4	4	5	26
Hardware or software token-based authentication	5	3	3	4	2	5	22
Aadhaar-linked biometric verification in relevant flows	4	3	3	4	5	4	23
Behavioural biometric plus step-up authentication	5	5	4	4	5	5	28

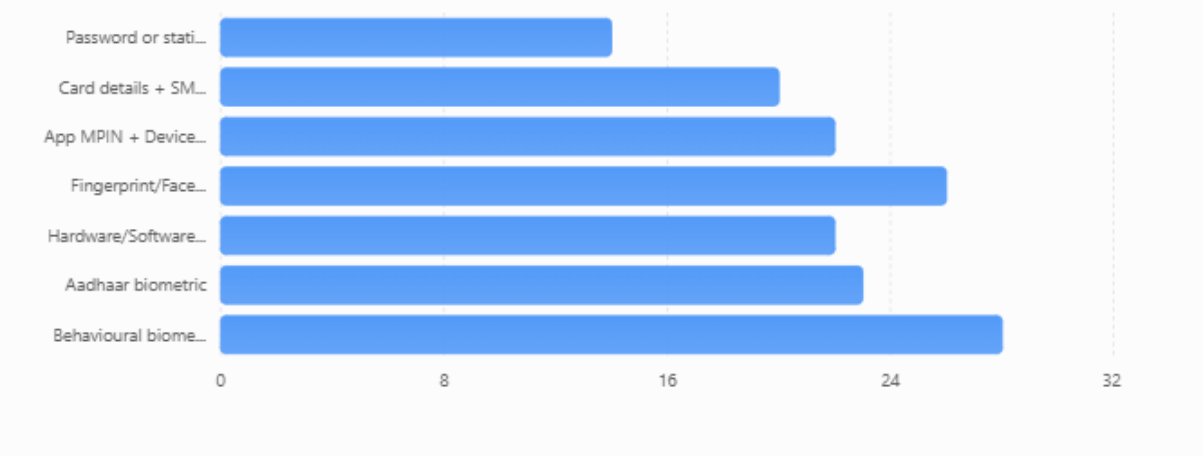

Figure: Numerical Comparison Table

7.3 Interpretation of the table

As can be seen in the table, behavioural biometric plus step-up authentication has the highest composite suitability score of 28/30. The result isn't because behavioural biometrics takes the place of all other factors, but because it is effective as part of a multi-layered architecture. They help to strengthen security without creating unnecessary friction, and they are compatible with having other checks based on risk as well. They are mainly weak in terms of risk for privacy exposure as these systems rely on the comprehensive capture and modelling of a user's behavior.

The device-native biometrics segment is also doing very well, with a score of 26 out of 30. They are easily understood, rapid and make sense in the smartphone ecosystems. The primary constraint is the difference in device capabilities, and the susceptibility of biometric information (Patil, 2025). Card information and SMS OTP score 20/30. This is a sign that OTP is not obsolete, it is still relevant and useful in the regulatory arena, but not optimal as the ecosystem's model. The Password or static pin only systems rate the lowest at 14 out of 30 as they are not adequate to address the current threats of remote payment fraud and do not match well with the RBI's expectation of multi factor authentication.

7.4 Emerging pattern across payment channels

The results indicate that payment channels will likely evolve to different mixes of authentication methods. In the future, the card-not-present ecommerce transactions are expected to shift towards issuers' more powerful risk assessment, tokenisation, and device recognition with OTP or biometric proof. The integration of device binding, in-app biometrics, and contextual anomaly detection will further bolster app-based authentication, which will be bolstered by UPI and mobile banking. For assisted and inclusion channels, simpler overt factors can be used, with background risk scoring and transaction-specific controls.

7.5 Regulatory fit and design implications

The exercise suggests the RBI's 2025 guidelines are flexible but are also weighted towards depth. Mechanisms that combine user-visible proof and contextual intelligence work best. Systems that are excessively dependent on any one factor type or on factor types that are easily changed by human activity do not fit as well (Lonkar *et al*., 2025). The idea of separate factors is important because false sense of security can be felt when designing at the surface level. An improperly designed collection of dependent signals is not as strong as a well-designed collection of independent signals.

8. Discussion

8.1 Why OTP is no longer enough

OTP is to the success of digital payments in India what the trifecto of cost, scale, and familiarity make it to the success of digital payments in the United States. A successful method can outlast the threat model that originally validated it, however. OTP is not weak due to the lack of transaction specificity, but because more and more attackers

are going after the channels and behaviors around it. Not all bad guys have to crack OTP cryptographically. They have to convince, capture, redirect or otherwise mislead the user when the OTP is used. The human layer is typically the weakest layer in a mass retail market.

The RBI guidelines are an indirect acknowledgment of this fact. The regulator's statement is a clear message to ecosystem players to break the perception of OTP as an all-in-one security paradigm (Krishna ES & Varghese James, 2026).The regulator's message is a definite warning to the players of the ecosystem that they should no longer see OTP as a security paradigm. OTP is just one of the tools and not the end goal of authentication design.

8.2 Why biometrics are attractive but incomplete

There are some problems that can be solved elegantly with biometrics. They eliminate memorization, decrease friction and make authentication more physical than ever. Native fingerprint and facial authentication can result in a more intuitive payment experience than reentering an OTP repeatedly in a smartphone environment. Some types of credential theft and credential reuse may also be prevented by the use of biometrics.

However, biometrics doesn't fit all solutions. The accuracy is dependent on the device and environment. Unlike OTP and PIN systems, they have different failure mode (Sharma, 2026)s. A stolen biometric template is a more serious problem in the long term than a stolen password. There are fairness and access issues, as well. Measuring payment authentication too strictly based on advanced device capabilities can lead to worse outcomes for portions of the population. Any large-scale biometric plan in India should thus involve a backup design, a policy of consent, retention and limited time and an accessible mechanism for redress.

8.3 Behavioural biometric as the next layer of authentication maturity

Behavioural biometric systems are significant because they move the act of authentication from individual points of verification to continuous verification of confidence. A classic payment flow requires the customer to be proven legitimate in one or two clear instances. A behavioural system detects uniformity throughout the whole session. This can be helpful for detecting remote computer fraud, scripted attacks, atypical navigation behaviour and non-standard use on the device.

This does not imply that behavioural biometrics should be rendered an unseen and unaccountable power. Indeed, the opacity that makes these systems predictive also poses regulatory risk. Institutions should be able to explain the role of the model in operational terms when it blocks or escalates transactions (Arunachalam, 2025). When there are too many false positives, it could hurt customer trust, particularly for new users, elderly users and users exhibiting irregular usage patterns. Behavioural biometric systems must therefore be used in addition to the ‘open' authentication and not as an ‘open' substitute for due process.

8.4 Privacy, surveillance, and governance concerns

The move from OTP to behavioural intelligence alters the privacy dynamics. OTP provides a fair amount of information other than possession of numbers and messages. Interaction signature, routine timing, mobility clues, device posture and usage patterns can be seen in behavioural biometrics. While these are being gathered to prevent fraud, they can end up in wider profiling. This means that governance is a key factor. The questions that arise from compliance are now data minimisation, purpose limitation, retention controls, separation of fraud analytics from commercial profiling, and disclosure to the user.

Relying on a compromise in which convenience is bought at the cost of transparency will not be the path forward for India's digital payments future. Advanced authentication's regulatory legitimacy will hinge on the proof of necessity, proportionality, and accountability of deployments by institutions.

8.5 Implications for financial inclusion

Payment systems cater to the needs of Indians with varying levels of literacy, device quality, language preferences, and disabilities. The widespread adoption of advanced biometrics or app-based authentication could benefit certain groups by enhancing fraud prevention, but at the same time be detrimental to others (Bandhela *et al*., 2024). The future architecture should thus be plural and layered, not singular. Low risk transactions can remain with a simple flow with background risk scoring. Biometric step-up or more substantial evidence may be required for high-risk events. Different controls might be required for channels and environments that are assisted or offline. Inclusion is NOT a zero-sum game with security; it is a security that must be reimagined in terms of user realities.

9. Conclusion

India's digital payment system now has evolved to the point that authentication can no longer be based on one most dominant element like SMS OTP. Older trust assumptions have proved to be insufficient in the age of digital commerce, where UPI and mobile channels play a key role and where fraud is increasingly complex. The RBI's authentication guidelines for 2025 offer a pertinent and significant regulatory framework for this transition. The directions ensure that the minimum two factor authentication is maintained, different factors are required, and the dynamic or proven proof is required for transactions with non-card-present digital payments, while also providing for the possibility of using extra risk-based checks. Medianama IBM

The findings of this paper indicate that while OTP is still a valuable but not enough tool for payment security, it needs to be complemented with other methods. While using device-native biometrics provide greater user binding and reduced friction, they are not without privacy, accessibility, and template security concerns. The most promising road toward adaptive and low- friction fraud control is behavioural biometrics, and

Reference

1. SAINI, A., 2025. SECURITY AND FRAUD PREVENTION IN ELECTRONIC PAYMENT SYSTEMS: UNDERSTANDING USER BEHAVIOUR. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S6 (2025): Posted 15 September), pp.727-739.
2. Vidani, J., 2024. A study on the rise and recent development in unified payments interface. *Available at SSRN 4849785*.
3. Agal, K., Mordhara, P.U., Patel, D., Rathod, H., Khandelwal, R. and Kadacha, N., Cybersecurity in Digital-Only Banks; How Entrepreneurs Are Shaping India's Digital Finance Ecosystem.
4. Khan, A.R., 2023. A Study of Consumer Behaviour in India with Respect to Digital Payments. *Available at SSRN 5383506*.
5. Khan, A.R., 2023. A Study of Consumer Behaviour in India with Respect to Digital Payments. *Available at SSRN 5383506*.
6. Khan, A.R., 2023. A Study of Consumer Behaviour in India with Respect to Digital Payments. *Available at SSRN 5383506*.
7. Quraishy, S.A., 2026. Digital Payment Systems: Their Role in Economic Growth and Associated Criminal Activities. *International Journal of Innovations in Science, Engineering And Management*, pp.113-119.
8. Jyothi, M.N., 2025. *An Evaluation of the Legal Framework of Electronic Banking with Special Reference to Data Protection and Cyber Security in India* (Doctoral dissertation, Alliance University (India)).
9. Jagannarayan, N., 2025. Digital Payments in India: Trends, Infrastructure, and Consumer Dynamics. *Lambart Academic Publication*.
10. Bhatnagar, P., Jain, D.K. and Agarwal, D.S., 2026. Unlocking the Gateways: A Comparative Study of Digital Payment Systems in India. *Available at SSRN 6426918*.
11. Vardhan, K., UPI and Digital Payments.
12. Bhatnagar, P., Jain, D.K. and Agarwal, D.S., 2026. Unlocking the Gateways: A Comparative Study of Digital Payment Systems in India. *Available at SSRN 6426918*.
13. Kaushik, L., 2026. *Digital Public Infrastructure-The Fundamentals of Building a Country's Digital Ecosystem*. Writer's Pocket.
14. Saraf, A.R., 2024. *How Developed is the Digital Payment in India* (Doctoral dissertation, Dublin, National College of Ireland).
15. Weerakoon, D., When "Security" Becomes Customer Punishment: A Critical Analysis of Sri Lankan Banking Apps, OTP Fatigue, and the Frictionless Fintech Imperative in 2026.
16. Majumdar, P., 2025. Implementing Aadhar-Linked Biometric Re-authentication Can Prevent Terrorist Misuse of India's Mobile Networks.
17. Kumar, P., Murmu, S., Chakraborty, A., Nath, A., Jee, K., Kaushal, A., Sharma, R. and Khan, F., 2026. Digital Payments Shaping Consumer Spending and Decision Making. In *Socially Responsible Approaches for Sustainable E-Commerce* (pp. 145-180). IGI Global Scientific Publishing.
18. Jagadisha, T., 2025. *Dynamics of Digital Economy in India*. AG Publishing House (AGPH Books).
19. Patil, A., 2025. Cybersecurity in Digital Payment Systems: Threats, Defenses, and Future Directions.
20. Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K. and Phadke, R.A., 2025. Tackling digital payment frauds: a study of consumer preparedness in India. *Journal of Financial Crime*, *32*(2), pp.257-278.
21. Krishna ES, A. and Varghese James, B., 2026. Digital Payments and Fraud Risk: Technological Innovations and Global Regulatory Responses. In *Financial Crime in the Digital Era: Innovative Approaches to Preventing Financial Fraud* (pp. 55-82). Cham: Springer Nature Switzerland.
22. Sharma, S., 2026. Artificial Intelligence-Enabled Secured Digital Payment Systems for Marketing Literacy of Urban and Rural Customers. In *Impacts of Digital Payment Systems on Marketing* (pp. 75-108). IGI Global Scientific Publishing.
23. Arunachalam, R.S., The Digital Trust Revolution–India's Cybersecurity Transformation in the Age of Unprecedented Financial Inclusion (2022–25). *Inclusive Finance India Report 2025*, p.147.

24. Bandhela, R.R., Kundavaram, R.R. and Onteddu, A.R., 2024. Enhancing Digital Wallet Payments through Data Analytics: A Study on Fraud Prevention and Personalized User Experience. *Journal of Computational Analysis and Applications*, *33*(2).
25. Ameer, S., Digital Financial Literacy, Overconfidence and Risky Behaviors: A Conceptual Framework for India's Digital Payments Era.
26. Choudhary, P., Das, S., Potta, M.P., Das, P. and Bichhawat, A., 2024, December. Online authentication habits of Indian users. In *2024 Conference on Building a Secure & Empowered Cyberspace (BuildSEC)* (pp. 66-73). IEEE.
27. Parameswaran, S., Gogia, Y., Williams, M.J., Nayak, R., Ashfaq, A. and Monica, L., 2024, March. Cardless society: Assessing the role of cardless atms in shaping the future of financial transactions. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. i-v). IEEE.
28. EREMEEVA, T. and AKULOVA, A., 2024. The european digital payment wallet ecosystem: key characteristics and insights.
29. SINGH, A.B., 2024. *A STUDY ON DIGITAL MONEY OF UPI (UNIFIED PAYMENTS INTERFACE) PAYMENT* (Doctoral dissertation, University of Mumbai).
30. SINGH, A.B., 2024. *A STUDY ON DIGITAL MONEY OF UPI (UNIFIED PAYMENTS INTERFACE) PAYMENT* (Doctoral dissertation, University of Mumbai).
31. Kacheru, G., 2025, October. Governance of AI-Enabled Behavioral Biometrics in Mobile Banking: Ensuring Security and Trust. In *2025 2nd International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT)* (pp. 1-6). IEEE.
32. Prabu, G., Nelson, G., Gowtham, M. and Yogesh, S., 2026, March. Enhancing UPI Transaction Security Through Colour Pattern Authentication. In *International Conference on Artificial Intelligence and Secure Data Analytics (ICAISDA 2025)* (pp. 276-285). Atlantis Press.
33. VENKATAIAH, G. and SAMBA, K., 2026. DIGITAL PAYMENT ADOPTION IN RURAL BANKING AT CANARA BANK. *Journal of Management Excellence*, *2*(1).
34. Sirigina, P.V., 2023. Digital Payment Security: A Developer Framework.
35. Chakkaa, N.B. and Saheba, S.S., Mobile payment fraud detection in UPIs through machine learning techniques: A systematic review.